Secrecy Capacity of Colored Gaussian Noise Channels With Feedback

Chong Li, *Member, IEEE*, Yingbin Liang, *Senior Member, IEEE*, H. Vincent Poor, *Fellow, IEEE*, and Shlomo Shamai (Shitz), *Life Fellow, IEEE*

***Abstract*— In this paper, the finite-order autoregressive moving average (ARMA) Gaussian wiretap channel with noiseless causal feedback is considered, in which an eavesdropper receives noisy observations of signals in both forward and feedback channels. It is shown that the generalized *Schalkwijk–Kailath* scheme, a capacity-achieving coding scheme for the Gaussian feedback channel, achieves the same maximum rate for the same channel even with the presence of an eavesdropper. Therefore, the secrecy capacity is equal to the feedback capacity without the presence of an eavesdropper for the Gaussian feedback channel. Furthermore, the results are extended to the additive white Gaussian noise (AWGN) channel with quantized feedback. It is shown that the proposed coding scheme achieves a positive secrecy rate. Our result implies that as the amplitude of the quantization noise decreases to zero, the secrecy rate converges to the capacity of the AWGN channel.**

***Index Terms*— Secrecy capacity, feedback, colored Gaussian, Schalkwijk-Kailath scheme.**

I. Introduction

IT HAS been more than a half century since information theorists began investigating the capacity of Gaussian feedback channels. As the pioneering studies on this topic, Shannon's 1956 paper [3] showed that feedback does not increase the capacity of the memoryless additive white Gaussian noise (AWGN) channel, and Elias [4], [5] proposed some simple corresponding feedback coding schemes. Then, Schalkwijk and Kailath [6], [7] developed a notable linear feedback coding scheme to achieve the capacity of the AWGN channel with feedback. Thereafter, the problem of finding the feedback capacity and capacity-achieving codes for Gaussian channels with memory, e.g., finite-order autoregressive moving average (ARMA) channels, has been extensively studied. Butman [8], [9], Wolfowitz [10], and Ozarow [11], [12] extended Schalkwijk's scheme [7] to finite-order Gaussian ARMA channels, leading to several valuable upper and lower bounds on the capacity. Motivated by these elegant results/insights, Cover and Pombra in their 1989 paper [13] made a breakthrough on characterizing the n-block capacity of the Gaussian feedback channel. In 2010, Kim [14] provided a characterization of the capacity of the finite-order Gaussian ARMA feedback channel (in the form of an infinite dimensional optimization problem) based on Cover-Pombra's n-block capacity characterization. Unfortunately, except for the first-order ARMA (i.e., ARMA(1)) noise channel, it is non-trivial to compute the capacity by solving this infinite dimensional optimization. Recently, Gattami [15] showed that the capacity of the stationary Gaussian noise channel with finite memory can be found by solving a semi-definite programming problem. In addition, Li and Elia [16] used control-theoretic tools to compute the capacity of finite-order ARMA Gaussian feedback channel and explicitly constructed capacity-achieving feedback codes.

As a natural extension of the above studies, understanding the finite-order ARMA Gaussian feedback channel with the presence of an eavesdropper (which has noisy access to the channel transmissions between legitimate users) is of great interest in the field of secure communication. Concretely, two fundamental questions can be asked:

1) would the feedback capacity of such a channel decrease subject to the secrecy constraint?
2) what would be the secrecy capacity-achieving codes?

Secure communication over feedback channels has attracted considerable attention in the last decade. Substantial progress has been made towards understanding this type of channels. Although the feedback may not increase the capacity of open-loop discrete memoryless channels (DMCs), in [17]–[28] it is showed that feedback can increase the secrecy capacity by sharing a secret key between legitimate users. In particular, in [17] and [18] the achievement of a positive secrecy rate is proved by using noiseless feedback even when the secrecy capacity of the forward channel is zero. In [20] the capacity of the DMC wiretap channel with a secure and rate-limited feedback link is studied, and a capacity-achieving coding scheme is provided for the class of physically degraded wiretap channels. In [21] it is proved that the judicious use of noisy feedback can increase the secrecy capacity to the capacity of

Manuscript received June 2, 2018; revised January 18, 2019; accepted February 25, 2019. Date of publication March 13, 2019; date of current version August 16, 2019. Y. Liang was supported in part by the U.S. National Science Foundation under Grant CCF-1801846. H. V. Poor was supported by the U.S. National Science Foundation under Grant CCF-093970 and Grant CCF-1513915. S. Shamai (Shitz) was supported by the European Union's Horizon 2020 Research and Innovation Programme under Grant 694630. This paper was presented in part at the 2017 and 2018 IEEE International Symposia on Information Theory [1], [2].

C. Li is with Nakamoto & Turing Labs, New York, NY 10018 USA (e-mail: chongl@ntlabs.io).

Y. Liang is with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43220 USA (e-mail: liang.889@osu.edu).

H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

S. Shamai (Shitz) is with the Department of Electrical Engineering, Technion–Israel Institute of Technology, Haifa 32000, Israel (e-mail: sshlomo@ee.technion.ac.il).

Communicated by M. Wigger, Associate Editor for Shannon Theory.

Digital Object Identifier 10.1109/TIT.2019.2904684

the source-destination channel in the absence of the wiretapper. In [22] a feedback scheme is proposed for the binary symmetric channel, which yields larger rate-equivocation regions and achievable secrecy rates. More importantly, the scheme can achieve a positive secrecy rate even when the eavesdropper's channel is less noisy than the legitimate channel. In [24] the model is considered in which the transmitter adds the transmitted signal with an interference signal generated by the legitimate receiver via the feedback link, and it is shown that if the transmit power is large enough a positive secrecy rate can be achieved even when the eavesdropper's channel is less noisy. In [25] the noiseless feedback wiretap channel is studied in which the legitimate channel is also informed with the channel state information in either a noncausal or causal manner. Also, in [26] the usefulness of noisy feedback is proved for a class of full-duplex two-way wiretap channels. Furthermore, in [27] an achievable scheme is presented for the wiretap channel with generalized feedback, which is a generalization and unification of several relevant previous results in the literature. Very recently, in [28] an improved feedback coding scheme is proposed for the wiretap channel with noiseless feedback, which is shown to outperform the existing ones in the literature.

The multiple-access (MA) and broadcast (BC) wiretap channels with feedback have also been studied in recent years. In [29] achievable secrecy rate regions are derived for the discrete memoryless Gaussian channels in which two trusted users send independent confidential messages to an intended receiver in the presence of a passive eavesdropper. In [30] inner and outer bounds on the secrecy rate region are developed for the MA wiretap channel with noiseless feedback. In [31] the secrecy capacity region of the broadcast channel with confidential messages (BC-CM) is characterized in which the legitimate receiver feeds back its received channel output to the transmitter via a noiseless feedback link. Furthermore, in [32] the broadcast wiretap channel with noiseless feedback is studied, and a new coding scheme is proposed which helps to increase the secrecy level for such a channel. In a more general setting where users have multiple-input multiple-output (MIMO) capability, in [33] the pre-log factor of the secrecy rate is characterized in the case with the number of antennas at the source being no larger than that at the eavesdropper. In [34] and [35], the benefits of state-feedback are investigated to increase the secrecy degrees of freedom for the two-user Gaussian MIMO wiretap channel.

However, it is noteworthy that most of the aforementioned results considered only *memoryless* wiretap channels. In this paper, we study the feedback wiretap channel with memory. More specifically, we make two major contributions:

1) We show that the feedback secrecy capacity C_{sc} of the finite-order ARMA Gaussian channel equals the feedback capacity C_{fb} of such a channel without the presence of an eavesdropper. Namely, $C_{sc} = C_{fb}$. Also, we propose a C_{sc}-achieving feedback coding scheme, which is a variant of the generalized *Schalkwijk-Kailath (S-K)* scheme. In other words, the secrecy is obtained without loss of the communication rate between legitimate users. This result can be viewed as an extension of the result in [19] which showed that the standard *S-K* scheme for the AWGN channel offers secrecy for free.
2) We further study the AWGN channel with quantized feedback, which is a more realistic channel model for the feedback link. We show that the proposed coding scheme provides non-trivial positive secrecy rates and achieves the feedback capacity of the AWGN channel as the amplitude of the quantization noise vanishes to zero.

The key idea to prove the main result $C_{sc} = C_{fb}$ comes from the following fact: after the first few transmissions, the generalized *S-K* scheme with the selected initializations can achieve C_{fb} by transmitting signals that depend only on the previous forward channel noise. As a consequence, the access to the noisiness of these signals (except the first few transmissions) provides zero information about the message to the eavesdropper, implying that the secrecy condition can be satisfied for legitimate users.

In addition, it is seen that the benefit of using feedback in the generalized *S-K* scheme is twofold: improving the decoding performance (i.e., doubly exponentially decaying error probability in decoding) and implicitly constructing a secret key (based on the forward channel noise extracted from the noiseless feedback signals) for secure transmissions. This fact, the twofold benefit of using feedback in secure communication, is aligned with the highlighted observations in [28].

The rest of the paper is organized as follows. Section II introduces the system model. Section III presents the main results of our paper. Section IV provides the technical proofs. Finally, Section V concludes the paper and outlines possible avenues for further research in this area.

Notation: Uppercase and the corresponding lowercase letters ($e.g.$, Y, Z, y, z) denote random variables and their realizations, respectively. We use log to denote the logarithm to base 2, and $0 \log 0 = 0$. We use $\mathbf{x}^{\mathbf{T}}$ to denote the transpose of a vector or a matrix $\mathbf{x}$. The notation V_a^b with integers a and b represents a sequence $\{V_a, V_{a+1}, \cdots, V_b\}$. $\mathbb{S}_X$ denotes the power spectral density of a time series $X(k)$ with time index k, and $\mathbb{Q}$ denotes the Fourier transform of filters in our problem. $\mathcal{RH}_2$ denotes the set of stable and proper rational filters in Hardy space $\mathcal{H}_2$.

II. System Model

In this section, we present the system model. First of all, we consider a discrete-time Gaussian channel with noiseless feedback as shown in Fig. 1. The additive Gaussian channel is modeled as

$$Y(k) = U(k) + W(k), \qquad k = 1, 2, \cdots, \tag{1}$$

where the Gaussian noise $\{W(k)\}_{k=1}^{\infty}$ is assumed to be stationary with power spectral density $\mathbb{S}_W(e^{j\theta})$ for $\forall \theta \in [-\pi, \pi)$. Unless the contrary is explicitly stated, "stationary" without specification refers to stationary in the wide sense. Moreover, we assume that the power spectral density satisfies the *Paley-Wiener* condition

$$\frac{1}{2\pi} \int_{-\pi}^{\pi} |\log \mathbb{S}_W(e^{j\theta})| d\theta < \infty.$$

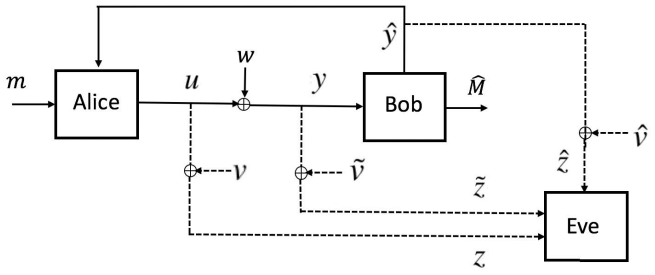

Fig. 1. Finite-order ARMA Gaussian wiretap channel with feedback.

Assumption 1. *(Finite-order ARMA Gaussian Channel) In this paper, the noise W is assumed to be the output of a finite-dimensional linear time invariant (LTI) minimum-phase stable system $\mathbb{H} \in \mathcal{RH}_2$, driven by white Gaussian noise with zero mean and unit variance. The power spectral density (PSD) of W is colored (nonwhite), bounded away from zero and has a canonical spectral factorization given by $\mathbb{S}_W(e^{j\theta}) = |\mathbb{H}(e^{j\theta})|^2$.*

As shown in Fig.1, the feedback wiretap channel of interest includes a forward channel from Alice to Bob as described by (1), a causal noiseless feedback $\hat{Y}$ from Bob to Alice, and three noisy observation channels to the eavesdropper Eve.

Assumption 2. *In this paper, the eavesdropper can access all three channel signals U, Y and $\hat{Y}$ with additive noises V, $\tilde{V}$ and $\hat{V}$, respectively. These noise processes are assumed to be stationary with finite memory and with strictly positive and bounded variances.*

The motivation of assuming such a powerful eavesdropper to access all three channel signals is that we aim to develop the strongest results by considering the worst case. Then, in practical scenarios in which the eavesdropper may have access to one of the three channel signals, or any combination of these signals, our results still hold. Note that a classical wiretap channel model can be recovered from our model if the eavesdropper's channel inputs from Y and $\hat{Y}$ are removed, and a degraded wiretap channel can be recovered if the eavesdropper's channel inputs from U and $\hat{Y}$ are removed. Mathematically, the noisy wiretap channels are modeled as

$$\begin{aligned} Z(k) &= U(k) + V(k), \\ \tilde{Z}(k) &= Y(k) + \tilde{V}(k), \\ \hat{Z}(k) &= \hat{Y}(k) + \hat{V}(k), \qquad k = 1, 2, \cdots. \end{aligned}$$

The additive noise processes V, $\tilde{V}$ and $\hat{V}$ are assumed to be arbitrarily finite-memory processes, i.e.,

$$\begin{aligned} p(v(k)|v_1^{k-1}) &= p(v(k)|v_{k-\bar{d}}^{k-1}), \qquad k \geq \bar{d}, \\ p(\tilde{v}(k)|\tilde{v}_1^{k-1}) &= p(\tilde{v}(k)|\tilde{v}_{k-\tilde{d}}^{k-1}), \qquad k \geq \tilde{d}, \\ p(\hat{v}(k)|\hat{v}_1^{k-1}) &= p(\hat{v}(k)|\hat{v}_{k-\hat{d}}^{k-1}), \qquad k \geq \hat{d}, \end{aligned} \tag{2}$$

where $\bar{d}$, $\tilde{d}$ and $\hat{d}$ respectively represent the sizes of the finite memories. Without loss of generality, we assume $\bar{d}$, $\tilde{d}$ and $\hat{d}$ are positive integers. All our results directly hold for the case of memoryless noises. In Assumption 2, we assume that these noise processes have strictly positive and bounded variances for all k. But they are not necessarily uncorrelated.

We specify a sequence of $(n, 2^{nR_s})$ channel codes with an achievable secrecy rate R_s as follows. We denote the message index by $m \in M$, which is uniformly distributed over the set $\{1, 2, 3, \cdots, 2^{nR_s}\}$. The encoding process $U_i(M, \hat{Y}^{i-1})$ at Alice satisfies the average transmit power constraint P, where $\hat{Y}^{i-1} = \{\hat{Y}_0, \hat{Y}_1, \cdots, \hat{Y}_{i-1}\}$ $(\hat{Y}_0 = \emptyset)$ for $i = 1, 2, \cdots, n$, and $U_1(M, \hat{Y}^0) = U_1(M)$. Bob decodes the message as $\hat{M}$ following a decoding function $g : Y_1^n \to \{1, 2, \cdots, 2^{nR_s}\}$ with an error probability satisfying

$$P_e^{(n)} = \frac{1}{2^{nR_s}} \sum_{m=1}^{2^{nR_s}} Pr(M \neq g(Y_1^n)|M = m) \leq \epsilon_n,$$

where $\lim_{n\to\infty} \epsilon_n = 0$. Meanwhile, the information about the message received by Eve should asymptotically vanish, i.e.,

$$\lim_{n\to\infty} \frac{1}{n} I(M; Z_1^n, \tilde{Z}_1^n, \hat{Z}_1^n) = 0.$$

The objective of secure communication is to send M to Bob at as high a rate R_s as possible within this secrecy constraint. The secrecy capacity C_{sc} is defined as the supremum of all achievable rates R_s. Mathematically,

$$\begin{aligned} C_{sc} = \sup_{\text{feasible coding schemes}} & R_s \\ s.t. \lim_{n\to\infty} \frac{1}{n} I(M; Z_1^n, \tilde{Z}_1^n, \hat{Z}_1^n) &= 0, \end{aligned} \tag{3}$$

where the argument "feasible coding schemes" refers to as all feedback codes that satisfy the secrecy requirements and the power constraint. Note that the feedback capacity (without the secrecy constraint) from Alice to Bob, denoted as C_{fb}, can be recovered by removing the secrecy constraint. This implies $C_{sc} \leq C_{fb}$.

III. Main Results

A. Feedback Capacity and Capacity-Achieving Coding Scheme

In this section, we review a characterization of the feedback capacity C_{fb} and then propose a variant of the generalized S-K scheme, which is a C_{fb}-achieving feedback code *without* the presence of an eavesdropper. The materials here are useful for us to further investigate the channel model with an eavesdropper.

First, under Assumption 1 Kim [14] showed that the feedback capacity from Alice to Bob with the average power budget $P > 0$ can be characterized by

$$\begin{aligned} C_{fb} = & \max_{\mathbb{Q}} \frac{1}{2\pi} \int_{-\pi}^{\pi} \log|1 + \mathbb{Q}(e^{i\theta})| d\theta, \\ s.t. \quad & \frac{1}{2\pi} \int_{-\pi}^{\pi} |\mathbb{Q}(e^{j\theta})|^2 \mathbb{S}_W(e^{j\theta}) d\theta \leq P, \\ & \mathbb{Q} \in \mathcal{RH}_2 \text{ is strictly causal.} \end{aligned} \tag{4}$$

Remark 1. *Under Assumption 1, the optimal $\mathbb{Q}$ has no zeros on the unit circle ([14, Proposition 5.1 (ii)]).*

Recent results in [16] provided a numerical approach to compute C_{fb} and explicitly constructed the optimal $\mathbb{Q}(e^{j\theta})$, which can be efficiently found by standard convex optimization tools. We refer the interested reader to [16] for details. In what follows, we describe, given an optimal $\mathbb{Q}$ in (4), how to construct an implementable coding scheme that achieves the feedback capacity from Alice to Bob.

First of all, once an optimal $\mathbb{Q}$ is found for the optimization problem in (4), we construct a feedback filter $\mathbb{K} = -\mathbb{Q}(1+\mathbb{Q})^{-1}$ stabilizing the channel within the prescribed input average power budget (see [16] for the proofs). Next, based on the transfer function $\mathbb{K}$, we construct an explicit feedback coding scheme as follows, which is deterministic (time-invariant) and has doubly exponentially decaying decoding error probability.

We first present the controller $\mathbb{K}$ as an LTI single-input-single-output (SISO) finite-dimensional discrete-time unstable system with the following state-space model:

$$\mathbb{K}: \quad \begin{bmatrix} X_s(k+1) \\ X_u(k+1) \end{bmatrix} = \begin{bmatrix} A_s & 0 \\ 0 & A_u \end{bmatrix} \begin{bmatrix} X_s(k) \\ X_u(k) \end{bmatrix} + \begin{bmatrix} B_s \\ B_u \end{bmatrix} Y(k)$$
$$U(k) = \begin{bmatrix} C_s & C_u \end{bmatrix} \begin{bmatrix} X_s(k) \\ X_u(k) \end{bmatrix}. \tag{5}$$

Based on Remark 1, we assume that the eigenvalues of A_u are strictly outside the unit disc while the eigenvalues of A_s are strictly inside the unit disc. Without loss of generality, we assume that A_s and A_u are in Jordan form. Assume A_u has d eigenvalues, denoted by $\lambda_i(A_u), i = 1, 2, \cdots, d$. Next, we propose a variant of the generalized S-K scheme (as shown in Fig. 2) which is equivalent to the the capacity-achieving coding scheme in [16] and [36] (as shown in Fig. 3). The proposed coding scheme decomposes $\mathbb{K}$ into an encoder (Alice) and a decoder (Bob) with the raw channel output fed back to the encoder via the noiseless feedback channel.

Decoder: The decoder runs dynamics driven by the channel output Y,

$$\hat{X}_u(k+1) = A_u \hat{X}_u(k) + B_u Y(k), \ \hat{X}_u(0) = 0.$$

It only produces an estimate of the initial condition of the encoder

$$\hat{M}(k) = A_u^{-k-1} \hat{X}_u(k+1).$$

Encoder: The encoder runs the following dynamics driven by the initial state, i.e., the message M:

$$\begin{aligned} \tilde{X}_u(k+1) &= A_u \tilde{X}_u(k), \ \tilde{X}_u(0) = M, \\ \tilde{U}_u(k) &= C_u \tilde{X}_u(k). \end{aligned}$$

It receives Y and runs dynamics driven by the received feedback Y,

$$\begin{aligned} X_s(k+1) &= A_s X_s(k) + B_s Y(k), \ X_s(0) = 0, \\ \hat{X}_u(k+1) &= A_u \hat{X}_u(k) + B_u Y(k), \ \hat{X}_u(0) = 0, \end{aligned}$$

and produces a signal

$$\hat{U}(k) = \begin{bmatrix} C_s & C_u \end{bmatrix} \begin{bmatrix} X_s(k) \\ \hat{X}_u(k) \end{bmatrix}.$$

Then, the encoder produces the channel input

$$U(k) = \tilde{U}_u(k) - \hat{U}(k).$$

The equivalence between the proposed coding scheme and the scheme in [16] (or [36]) can be directly verified by comparing the channel inputs U (encoder) and the estimate of the message $\hat{M}$ (decoder) of the two schemes. Thus, we only present this result as follows and omit the trivial proof.

Proposition 1. *For a given message M and a sequence of additive noise W_1^k ($k \geq 1$), the coding schemes in Fig. 2 and Fig. 3 produce identical channel input $U(k)$ and message estimate $\hat{M}(k)$ for $\forall k$.*

Remark 2. *It is important to note that the "equivalence" only holds for such a channel without an eavesdropper. This is because in our model the eavesdropper can access the feedback link. In the proposed coding scheme, since the channel output is directly fed back to Alice, the eavesdropper's access to both the channel output and the feedback link is no different from its access to the channel output only. However, this is clearly not true for the coding scheme in Fig. 3, in which the eavesdropper can extract more useful information from the decoding process in Bob by having access to the feedback link. In fact, this is the motivation for us to propose the coding scheme in Fig. 2 for secure communication.*

With a bit abuse of notation, in the above coding scheme we use notation $M \in \mathbb{R}^d$ to represent the underlying message which is allocated at the centroid of a unit hypercube in the coordinate system depending on $A_u \in \mathbb{R}^{d \times d}$. We refer the interested readers to [36, Th. 4.3] for detailed explanation. For a scalar $A_u \in \mathbb{R}$, the unit hypercube becomes an interval, e.g., $[-\frac{1}{2}, \frac{1}{2}]$. That is, 2^{nR_s} messages are represented by the middle signal points of equally divided 2^{nR_s} subintervals within $[-\frac{1}{2}, \frac{1}{2}]$. In the rest of the paper, we use M to represent the signal point of the messages rather than the message index.

In the next section, we show that the proposed coding scheme with the selected initializations can lead to the asymptotic zero leakage of the message to Eve. This implies $C_{sc} = C_{fb}$.

B. Secrecy Capacity of the Finite-Order ARMA Feedback Gaussian Channel with an Eavesdropper

We first present some necessary properties of the proposed coding scheme without the presence of an eavesdropper. We then use these properties to establish our main theorem which characterizes the feedback secrecy capacity and an achieving coding scheme.

The following result shows that, by choosing the particular d-step initializations (in the state-space representation) for the proposed coding scheme, the channel inputs ($k \geq d+1$) are determined only by the past additive Gaussian noise W, a fact that is vital to guarantee the asymptotic secrecy from Eve.

Proposition 2. *For the feedback coding scheme in Fig. 2, assume the first d-step channel inputs $U_1^d = A_u^{d+1} M$ (where A_u^{d+1} refers to matrix A_u to the power $d+1$), the dynamics*

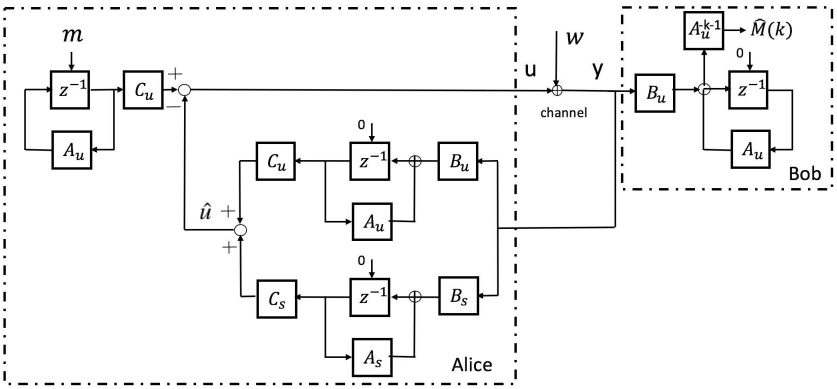

Fig. 2. A variant of the generalized *S-K* scheme. The scheme is represented under z-transform in which z^{-1} represents the one-step delay in time domain.

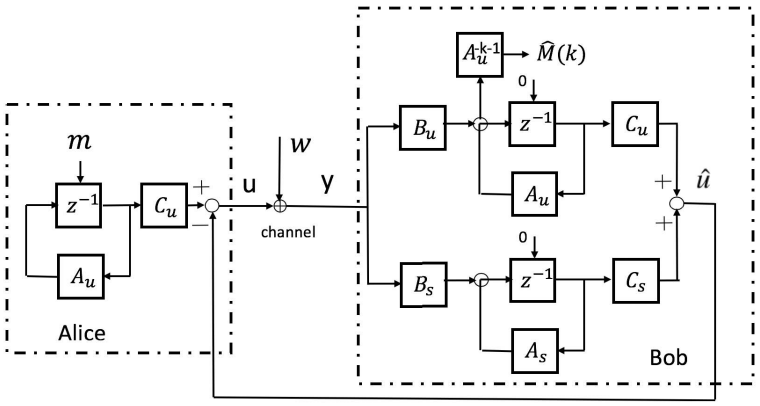

Fig. 3. Capacity-achieving coding scheme in [16] and [36].

$\hat{X}_u(d+1) = Y_1^d$ *(or equivalently, the estimated message* $\hat{M}(d) = A_u^{-d-1}Y_1^d$*) and* $X_s(d+1) = 0$*, where* d *is the number of eigenvalues of the matrix* A_u*. Then the induced channel inputs* $U(k)$ *for* $k \geq d+1$ *are determined only by the past Gaussian noise* W_1^{k-1}.

Proof. See Section IV-A. □

Proposition 3. *With the initializations defined in Proposition 2, the proposed coding scheme in Fig. 2 remains* C_{fb}*-achieving.*

Proof. The proof follows directly from two facts. On the one hand, all these initializations have no effect on the average transmission power on channel inputs, which depend only on the steady state of the underlying LTI systems. Further, these initializations do not change the reliable transmission rate of the coding scheme $\mathbb{K}$, which is defined asymptotically and is determined only by the unstable eigenvalues in A_u [36]. □

It is noteworthy that the above propositions implicitly reveal an interesting behavior of the proposed coding scheme $\mathbb{K}$ with the selected initializations. Specifically, in the first d-step, Alice transmits a (scaled) message while Bob receives a noisy (unbiased) message. In the sequential steps, Alice sends projected values of the past noise (shared key with Bob) to refine Bob's estimate. In the meanwhile, Eve receives only the noisy refinements from Alice due to the additive noises V, $\tilde{V}$ and $\hat{V}$ on the eavesdropper channels. The next theorem establishes that the noisiness of these refinements for Eve leads to the asymptotic ignorance of the message.

Theorem 1. *Consider the finite-order ARMA Gaussian wiretap channel with feedback (Fig. 1) under the average channel input power constraint* $P > 0$*. Then,*

1) *the feedback secrecy capacity equals the feedback (Shannon) capacity, i.e.,* $C_{sc} = C_{fb}$*; and*
2) *the feedback secrecy capacity is achieved by the proposed* C_{fb}*-achieving feedback coding scheme* $\mathbb{K}$ *with* $U_1^d = A_u^{d+1}M$*,* $\hat{X}_u(d+1) = Y_1^d$ *(i.e., the estimated message* $\hat{M}(d) = A_u^{-d-1}Y_1^d$*), and* $X_s(d+1) = 0$.

Proof. See Section IV-B. □

Remark 3. *For the finite-alphabet DMCs with the channel input* X*, the channel output* Y *and the eavesdropper's received signal* Z*, Ahlswede and Cai [31] derived the secrecy capacity of a wiretap channel with feedback as*

$$C_{sc} = \max_{p(x)} \min\{H(Y|Z), I(X;Y)\}. \tag{6}$$

Note that the above result holds even for the non-degraded wiretap channel (i.e., Markov chain $X \to Z \to Y$*) with noiseless link* $X \to Z$*, which corresponds to our model with Eve's noise* $V = 0$*. However, the proof of Theorem* 1 *shows*

that our proposed linear coding scheme leads to zero rate if $V = 0$. That is, although our capacity-achieving coding scheme gains simplicity (i.e., linearity) and superior performance (i.e., doubly exponentially decaying error probability in decoding), it is not robust to the noise-free eavesdropper as a result of such a simple coding structure.

In addition, for both finite and continuous-alphabet DMCs, Ardestanizadeh et al. [20] showed that the secrecy capacity of a degraded wiretap channel with a secure feedback link of a rate R_f is given by

$$C_{sc} = \max_{p(x)} \min\{I(X;Y), I(X;Y|Z) + R_f\}. \tag{7}$$

It is noteworthy that the above two capacity results for DMCs cannot be easily extended to wiretap channel with memory. Specifically, it is known that the feedback capacity of channels with memory (including colored Gaussian channels) has been proved to be characterized by the directed information [37], [38], which is a quantity no larger than mutual information. However, the characterization for the feedback capacity of wiretap channels with memory is unknown till now. Surprisingly Theorem 1 implies that the secrecy capacity for the colored Gaussian channels can also be characterized by the directed information. But extensions to other feedback wiretap channels with memory are technically nontrivial.

Remark 4. *According to the term $H(Y|Z)$ in Ahlswede's result (6), it is concluded that for finite-alphabet DMCs the secrecy capacity depends on the variance of Eve's noise. Roughly speaking, the capacity converges to zero as Eve's noise becomes sufficiently small. But this conclusion may not hold for continuous noises. On the one hand, Ahlswede's result (6) does not apply since the differential entropy $h(Y|Z)$ could be negative for continuous variables. On the other hand, following the proof of Theorem 1, one can see that $C_{sc} = C_{fb}$ is always true provided that none of the variances of Eve's noises $V, \hat{V}$ and $\tilde{V}$ is zero. This is because according to Proposition 2 our coding scheme essentially extracts fresh randomness (i.e., the continuous forward channel noise W) from the feedback output symbols and uses that randomness as a key. However, because Eve's noise (even arbitrarily small) is added to the continuous noise W in every channel use, this randomness (or secret key) is hidden from Eve. Furthermore, when specified to a degraded wiretap AWGN channel, as presented in the following corollary, our result becomes $C_{sc} = C_{fb} = \max_{p(x)} I(X;Y)$.* [1] *Considering the degraded wiretap channel with feedback, this result is consistent with (7) with $R_f = \infty$ (corresponding to the noiseless feedback), which also implies that the secrecy capacity does not depend on Eve's noise (as long as the variance of Eve's noise is nonzero).*

The next corollary shows that the well-known *S-K* scheme [7] is a special case of our proposed coding scheme.

Corollary 1. *Consider the AWGN wiretap channel with feedback (Fig. 1) under the average channel input power constraint $P > 0$. Assume that the additive noise W has mean zero and variance $\sigma_w^2 > 0$. Then the proposed coding scheme with $A_u = \sqrt{\frac{P+\sigma_w^2}{\sigma_w^2}}$, $B_u = -\frac{\sqrt{A_u^2-1}}{A_u}$, $C_u = -\sqrt{A_u^2-1}$, and $A_s = B_s = C_s = 0$ becomes the original S-K scheme, and achieves the secrecy capacity $C_{sc} = C_{fb} = \frac{1}{2}\log(1+\frac{P}{\sigma_w^2})$.*

Proof. See Section IV-C. □

This corollary recovers [19, Th. 5.1], showing that the well-known *S-K* scheme not only achieves the feedback capacity but also automatically provides the secrecy from the eavesdropper.

C. Feedback With Quantization Noise

In this section, we extend our result to Gaussian channels with quantized feedback. It is noteworthy that the capacity of colored Gaussian channels with noisy feedback remains an open problem [39], [40], even when simplified to quantized feedback. Therefore, in this paper, as an initial step towards understanding the secrecy capacity of noisy Gaussian feedback channels, we focus on AWGN channels with quantized feedback. Martins and Weissman [41] presented a linear coding scheme featuring a positive information rate and a positive error exponent for AWGN channels with feedback corrupted by quantization or bounded noise. In what follows, we show that our proposed *linear* coding scheme, when specified to the AWGN channel with quantized feedback, converges to the scheme in [41] and, more importantly, leads to a positive secrecy rate. Furthermore, this achievable secrecy rate converges to the capacity of the AWGN channel as the amplitude of the quantization noise decreases to zero.

Firstly, we define a memoryless uniform quantizer with sensitivity σ_q as follows.

Definition 1. *[41] Given a real parameter $\sigma_q > 0$, a uniform quantizer with sensitivity σ_q is a function $\Phi_{\sigma_q}: \mathbb{R} \to \mathbb{R}$ defined as*

$$\Phi_{\sigma_q}(Y) = 2\sigma_q \lfloor \frac{Y+\sigma_q}{2\sigma_q} \rfloor,$$

where $\lfloor \cdot \rfloor$ represents the floor function. The quantization error at instant k, i.e., the feedback noise, is given by

$$Q(k) = \Phi_{\sigma_q}(Y(k)) - Y(k).$$

Note that, for a given channel output $Y(k)$, the quantization noise $Q(k)$ can be recovered by the decoder as we assume the decoder knows the quantization rule. In other words, the decoder can get access to both the channel outputs and the feedback noise while the encoder can only get access to the corrupted channel output. On the other hand, note that with the quantized feedback the proposed coding scheme and the coding scheme in [16] and [36] (as shown in Fig. 3) are no longer equivalent due to the different feedback signals. As a consequence, the coding scheme in [16] and [36] may not be applicable here. We next tailor our proposed coding scheme to the AWGN channel with quantized feedback as follows (see Fig. 4). We first let $A_s = B_s = C_s = 0$.

[1] For the AWGN channel, the feedback capacity equals the capacity without feedback which is characterized by the mutual information.

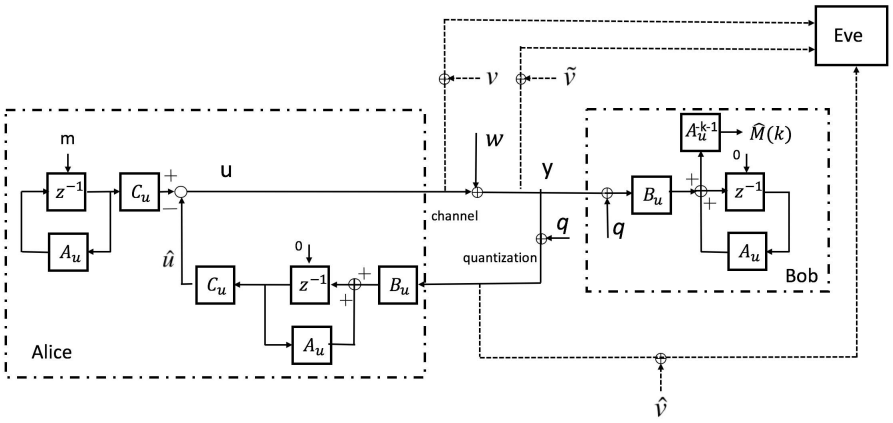

Fig. 4. Coding structure for the AWGN channel with quantized feedback. The quantization noise q can be recovered by the decoder to help decoding.

Decoder: The decoder runs dynamics driven by the sum of the channel output Y and the quantization noise Q as follows,

$$\hat{X}_u(k+1) = A_u\hat{X}_u(k) + B_u(Y(k)+Q(k)),\ \hat{X}_u(0)=0.$$

It produces an estimate of the initial condition of the encoder, as given by

$$\hat{M}(k) = A_u^{-k-1}\hat{X}_u(k+1).$$

Encoder: The encoder runs the following dynamics:

$$\tilde{X}_u(k+1) = A_u\tilde{X}_u(k),\ \tilde{X}_u(0)=M,$$
$$\tilde{U}_u(k) = C_u\tilde{X}_u(k).$$

It receives $Y+Q$ and duplicates the decoding dynamics,

$$\hat{X}_u(k+1) = A_u\hat{X}_u(k) + B_u(Y(k)+Q(k)), \hat{X}_u(0)=0,$$

and produces a signal,

$$\hat{U}(k) = C_u\hat{X}_u(k).$$

Then, it produces the channel input

$$U(k) = \tilde{U}_u(k) - \hat{U}(k).$$

We next show that the above coding scheme can achieve a positive secrecy rate, which converges to the AWGN capacity as the feedback noise σ_q decreases. The following definition is used to characterize this secrecy rate.

Definition 2. *[41] For the given positive real parameters σ_w, σ_q and P, define a parameter r_q as follows.*

1) *If $4\sigma_q \le P$, r_q is the nonnegative real solution of the following equation,*

$$\sigma_w\sqrt{2^{2r_q}-1} = \sqrt{P} - \sigma_q(1+2^{r_q}).$$

2) *If $4\sigma_q > P$, then $r_q = 0$.*

It is easy to check that r_q satisfies the following three properties [41]:

1) r_q converges to the AWGN capacity as σ_q decreases, i.e.,

$$\lim_{\sigma_q\to 0^+} r_q = \frac{1}{2}\log(1+\frac{P}{\sigma_w^2}).$$

2) If $\sigma_q = \frac{\sqrt{P}}{2}$, we have $r_q = 0$.
3) If $P \gg \max\{\sigma_w^2, \sigma_q^2\}$, $r_q \simeq \log(\frac{\sqrt{P}}{\sigma_w+\sigma_q})$. In other words, the ratio of r_q and $\log(\frac{\sqrt{P}}{\sigma_w+\sigma_q})$ converges to 1 as $P\to\infty$.

Theorem 2. *Consider the AWGN channel with memoryless uniformly quantized feedback defined in Definition 1, where the channel input power constraint is $P>0$, and the noise variance of the AWGN channel and the quantization sensitivity in the feedback link are assumed to be σ_w^2 and σ_q, respectively. Assume $U(1) = A_u^2M$, and $\hat{X}_u(2) = Y(1)+Q(1)$ (or equivalently, $\hat{M}(1) = A_u^{-2}(Y(1)+Q(1))$). Then, the above proposed coding scheme with $A_u = 2^r, B_u = -1, C_u = \frac{1}{Au} - A_u$ and $A_s = B_s = C_s = 0$ achieves a secrecy rate r for all $r < r_q$ (r_q is defined in Definition 2).*

Proof. See Section IV-D. □

Combined with the first property on r_q in Definition 2, this theorem implies that the achievable feedback secrecy rate of the proposed coding scheme converges to the AWGN capacity as σ_q decreases to zero.

IV. Technical Proofs

In this section, we present the proofs of the results in Section III.

A. Proof of Proposition 2

Based on the proposed coding scheme, we have

$$\begin{aligned}U(k) =& \tilde{U}_u(k) - \hat{U}(k)\\ =& C_u(\tilde{X}_u(k) - \hat{X}_u(k)) - C_sX_s(k)\\ =& C_u(A_u\tilde{X}_u(k-1) - A_u^k\hat{M}(k-1)) - C_sX_s(k)\\ =& \cdots\\ =& C_u(A_u^kM - A_u^k\hat{M}(k-1)) - C_sX_s(k)\\ =& C_uA_u^k(M-\hat{M}(k-1)) - C_sX_s(k). \end{aligned} \tag{8}$$

Next, for $k \ge d+1$, i.e., the initial d transmissions are complete, the signals start to evolve as described in the

proposed coding scheme. Specifically,

$$\begin{aligned}
&\hat{M}(k)\\
=&A_u^{-k-1}\hat{X}_u(k+1)\\
=&A_u^{-k-1}(A_u\hat{X}_u(k)+B_uY(k))\\
=&A_u^{-k}\hat{X}_u(k)+A_u^{-k-1}B_uY(k)\\
=&\hat{M}(k-1)+A_u^{-k-1}B_uY(k)\\
=&\hat{M}(k-1)+A_u^{-k-1}B_u(U(k)+W(k))\\
\overset{(a)}{=}&\hat{M}(k-1)+A_u^{-k-1}B_u(C_uA_u^kM-C_uA_u^k\hat{M}(k-1)\\
&-C_sX_s(k)+W(k))\\
=&\hat{M}(k-1)-A_u^{-k-1}B_uC_uA_u^k\hat{M}(k-1)\\
&+A_u^{-k-1}B_uC_uA_u^kM+A_u^{-k-1}B_u(W(k)\\
&-C_sX_s(k))+M-M\\
=&(I-A_u^{-k-1}B_uC_uA_u^k)\hat{M}(k-1)\\
&-(I-A_u^{-k-1}B_uC_uA_u^k)M\\
&+A_u^{-k-1}B_u(W(k)-C_sX_s(k))+M\\
=&(I-A_u^{-k-1}B_uC_uA_u^k)(\hat{M}(k-1)-M)\\
&+A_u^{-k-1}B_u(W(k)-C_sX_s(k))+M,
\end{aligned}\tag{9}$$

where step (a) follows from (8). Let $\alpha_k = I - A_u^{-k-1}B_uC_uA_u^k$ and $\beta_k = A_u^{-k-1}B_u$. Moving M to the left side, we have

$$\hat{M}(k)-M=\alpha_k(\hat{M}(k-1)-M)+\beta_k(W(k)-C_sX_s(k)).$$

By iterating the above equation, for $k \geq d+1$, we obtain

$$\begin{aligned}
\hat{M}(k)-M=&\prod_{i=d+1}^{k}\alpha_i(\hat{M}(d)-M)\\
&+\sum_{i=d+1}^{k}\prod_{j=i+1}^{k}\alpha_j\beta_i(W(i)-C_sX_s(i)),
\end{aligned}$$

where we assume $\alpha_{k+1}=1$. Given $U_1^d = A_u^{d+1}M$ and $\hat{M}(d)=A_u^{-d-1}Y_1^d$, we have

$$\hat{M}(d)=A_u^{-d-1}(U_1^d+W_1^d)=M+A_u^{-d-1}W_1^d.$$

Then, this yields

$$\begin{aligned}
\hat{M}(k)-M=&\prod_{i=d+1}^{k}\alpha_iA_u^{-d-1}W_1^d\\
&+\sum_{i=d+1}^{k}\prod_{j=i+1}^{k}\alpha_j\beta_i(W(i)-C_sX_s(i)).
\end{aligned}$$

Now, we derive the channel inputs $U(k)$ for $k \geq d+1$. Firstly, for $k=d+1$, given $X_s(d+1)=0$, from (8) we have

$$\begin{aligned}
U(d+1)=&-C_uA_u^{d+1}(\hat{M}(d)-M)-C_sX_s(d+1)\\
=&-C_uA_u^{d+1}(\hat{M}(d)-M)\\
=&-C_uW_1^d.
\end{aligned}\tag{10}$$

Then, for $k \geq d+2$, we present the channel inputs $U(k)$ and recall the evolution of $X_s(k)$ as follows:

$$\begin{aligned}
U(k)=&-C_uA_u^k(\hat{M}(k-1)-M)-C_sX_s(k)\\
=&-C_uA_u^k\Bigg(\prod_{i=d+1}^{k-1}\alpha_iA_u^{-d-1}W_1^d\\
&+\sum_{i=d+1}^{k-1}\prod_{j=i+1}^{k-1}\alpha_j\beta_i(W(i)-C_sX_s(i))\Bigg)-C_sX_s(k),
\end{aligned}$$

and

$$\begin{aligned}
X_s(k)=&A_sX_s(k-1)+B_s(U(k-1)+W(k-1)).
\end{aligned}\tag{11}$$

Starting with $U(d+1)=-C_uW_1^d$ and $X_s(d+1)=0$, one can see that the above coupled iterations induce values of $U(k)$ and $X_s(k)$ that depend only on the additive noise W_1^{k-1}. Therefore, for $k \geq d+2$,

$$U(k)\triangleq\phi_k(W_1^{k-1}),\tag{12}$$

where the mapping $\phi_k:\mathbb{R}^{k-1}\to\mathbb{R}$ is defined by the iterations in (11). Combining with (10), we conclude that, for $k \geq d+1$, $U(k)$ depends only on W_1^{k-1}. The proof is complete.

B. Proof of Theorem 1

First of all, since the proposed coding scheme derived from the optimal filter $\mathbb{Q}$ is equivalent to the capacity-achieving coding scheme in [16] and [36], it also achieves the feedback capacity C_{fb}. Then, in what follows, we need only to show that under the selected initializations of the proposed coding scheme, the following secrecy requirement is satisfied:

$$\lim_{n\to\infty}\frac{1}{n}I(M;Z_1^n,\tilde{Z}_1^n,\hat{Z}_1^n)=0.$$

Following from the model in Fig. 1, and (10) and (12) in the proof of Proposition 2, and the selected initializations $U_1^d = A_u^{d+1}M$, the three inputs $Z(k)$, $\tilde{Z}(k)$ and $\hat{Z}(k)$ to Eve for $k \geq 1$ are given by

$$\begin{aligned}
Z_1^d=&U_1^d+V_1^d=A_u^{d+1}M+V_1^d,\\
Z(d+1)=&U(d+1)+V(d+1)\\
=&-C_uW_1^d+V(d+1),\\
Z(k)=&\phi_k(W_1^{k-1})+V(k),\quad k\geq d+2,
\end{aligned}\tag{15}$$

$$\begin{aligned}
\tilde{Z}_1^d=&U_1^d+\tilde{V}_1^d+W_1^d=A_u^{d+1}M+\tilde{V}_1^d+W_1^d,\\
\tilde{Z}(d+1)=&U(d+1)+\tilde{V}(d+1)+W(d+1)\\
=&-C_uW_1^d+\tilde{V}(d+1)+W(d+1),\\
\tilde{Z}(k)=&\phi_k(W_1^{k-1})+\tilde{V}(k)+W(k),\quad k\geq d+2,
\end{aligned}\tag{16}$$

and

$$\begin{aligned}
\hat{Z}_1^d=&U_1^d+\hat{V}_1^d+W_1^d=A_u^{d+1}M+\hat{V}_1^d+W_1^d,\\
\hat{Z}(d+1)=&U(d+1)+\hat{V}(d+1)+W(d+1)\\
=&-C_uW_1^d+\hat{V}(d+1)+W(d+1),\\
\hat{Z}(k)=&\phi_k(W_1^{k-1})+\hat{V}(k)+W(k),\quad k\geq d+2.
\end{aligned}\tag{17}$$

$$
\begin{aligned}
H(M|Z_1^n, \tilde{Z}_1^n, \hat{Z}_1^n) &\overset{(a)}{\geq} H(M|Z_1^n, \tilde{Z}_1^n, \hat{Z}_1^n, W_1^n, V_{d+1}^n, \tilde{V}_{d+1}^n, \hat{V}_{d+1}^n) \\
&\overset{(b)}{=} H(M|Z_1^d, \tilde{Z}_1^d, \hat{Z}_1^d, W_1^n, V_{d+1}^n, \tilde{V}_{d+1}^n, \hat{V}_{d+1}^n) \\
&\overset{(c)}{=} H(M|A_u^{d+1}M + V_1^d, A_u^{d+1}M + \tilde{V}_1^d + W_1^d, A_u^{d+1}M + \hat{V}_1^d + W_1^d, W_1^n, V_{d+1}^n, \tilde{V}_{d+1}^n, \hat{V}_{d+1}^n) \\
&= H(M|A_u^{d+1}M + V_1^d, A_u^{d+1}M + \tilde{V}_1^d, A_u^{d+1}M + \hat{V}_1^d, W_1^n, V_{d+1}^n, \tilde{V}_{d+1}^n, \hat{V}_{d+1}^n) \\
&\overset{(d)}{=} H(M|A_u^{d+1}M + V_1^d, A_u^{d+1}M + \tilde{V}_1^d, A_u^{d+1}M + \hat{V}_1^d, W_1^n, V_{d+1}^{d+\bar{d}}, \tilde{V}_{d+1}^{d+\tilde{d}}, \hat{V}_{d+1}^{d+\hat{d}}) \\
&= H(M|A_u^{d+1}M + V_1^d, A_u^{d+1}M + \tilde{V}_1^d, A_u^{d+1}M + \hat{V}_1^d, V_{d+1}^{d+\bar{d}}, \tilde{V}_{d+1}^{d+\tilde{d}}, \hat{V}_{d+1}^{d+\hat{d}}), \qquad (13)
\end{aligned}
$$

$$
\begin{aligned}
I(M; Z_1^n, \tilde{Z}_1^n, \hat{Z}_1^n) &= H(M) - H(M|Z_1^n, \tilde{Z}_1^n, \hat{Z}_1^n) \\
&\leq H(M) - H(M|A_u^{d+1}M + V_1^d, A_u^{d+1}M + \tilde{V}_1^d, A_u^{d+1}M + \hat{V}_1^d, V_{d+1}^{d+\bar{d}}, \tilde{V}_{d+1}^{d+\tilde{d}}, \hat{V}_{d+1}^{d+\hat{d}}) \\
&= I(M; A_u^{d+1}M + V_1^d, A_u^{d+1}M + \tilde{V}_1^d, A_u^{d+1}M + \hat{V}_1^d, V_{d+1}^{d+\bar{d}}, \tilde{V}_{d+1}^{d+\tilde{d}}, \hat{V}_{d+1}^{d+\hat{d}}) \\
&= I(M; \mathbb{A}M + \mathbb{B}), \qquad (14)
\end{aligned}
$$

Recall that $V(k)$, $\tilde{V}(k)$ and $\hat{V}(k)$ are additive noise processes defined in (2).

Then, for $n \geq d + \max\{\bar{d}, \tilde{d}, \hat{d}\} + 1$, we have (13), as shown at the top of this page, where step (a) follows from the fact that conditioning does not increase entropy; steps (b) and (c) follow from (15), (16) and (17); step (d) follows from the finite memory of the wiretap channel noise processes $(V, \tilde{V}, \hat{V})$; and the last step follows from the fact that the noise W is assumed to be independent of the other variables.

Then, we obtain (14), as shown at the top of this page, where $\mathbb{A} = [A_u^{d+1}, A_u^{d+1}, A_u^{d+1}, \mathbf{0}^T]$ ($\mathbf{0}$ is an $(\bar{d} + \tilde{d} + \hat{d}) \times d$ zero matrix) and $\mathbb{B} = [V_1^d, \tilde{V}_1^d, \hat{V}_1^d, V_{d+1}^{d+\bar{d}}, \tilde{V}_{d+1}^{d+\tilde{d}}, \hat{V}_{d+1}^{d+\hat{d}}]$. Recall that the message M is uniformly selected from the index set $\{1, 2, \cdots, 2^{nR_s}\}$ which correspond to points equally spaced in a d-dimensional unit hypercube. The covariance matrix of M is given by $\frac{1}{12} I_d$ as $n \to \infty$. Following from the fact that for a fixed covariance, a vector Gaussian input distribution maximizes the mutual information, we obtain the following upper bound:

$$
\begin{aligned}
&\lim_{n\to\infty} \frac{1}{n} I(M; Z_1^n, \tilde{Z}_1^n, \hat{Z}_1^n) \\
&\overset{(a)}{\leq} \lim_{n\to\infty} \frac{1}{n} I(M; \mathbb{A}M + \mathbb{B}) \\
&= \lim_{n\to\infty} \frac{1}{n} \Big(h(\mathbb{A}M + \mathbb{B}) - h(\mathbb{A}M + \mathbb{B}|M) \Big) \\
&= \lim_{n\to\infty} \frac{1}{n} \Big(h(\mathbb{A}M + \mathbb{B}) - h(\mathbb{B}) \Big) \\
&\overset{(b)}{\leq} \lim_{n\to\infty} \frac{1}{2n} \log\det \left(E[\mathbb{B}\mathbb{B}^T] + \frac{1}{12}\mathbb{A}\mathbb{A}^T \right) - \frac{1}{n} h(\mathbb{B}) \\
&= \lim_{n\to\infty} \frac{1}{n} \left[\frac{1}{2} \log\det \left(E[\mathbb{B}\mathbb{B}^T] + \frac{1}{12}\mathbb{A}\mathbb{A}^T \right) - h(\mathbb{B}) \right] \\
&\overset{(c)}{=} 0, \qquad (18)
\end{aligned}
$$

where step (a) follows from (14), and step (b) follows due to the maximum entropy property of the Gaussian distribution. For the last step (c), we note that, given that $\mathbb{B}$ is a vector of noises with bounded variances, the entropy $h(\mathbb{B})$ and the covariance matrix $E[\mathbb{B}\mathbb{B}^T]$ are bounded and independent of the index n. In addition, $\mathbb{A}$ is a deterministic matrix constructed in the coding scheme. Therefore, the term $\frac{1}{2} \log\det \left(E[\mathbb{B}\mathbb{B}^T] + \frac{1}{12}\mathbb{A}\mathbb{A}^T \right) - h(\mathbb{B})$ is bounded and independent of the index n and hence dividing such a bounded term by n converges to zero as n goes to infinity. The proof is complete.

C. Proof of Corollary 1

Based on Schalkwijk's scheme in [7], the channel input (encoder) and the message estimate (decoder) for $k = 1$ are given below with the notations used in this paper.

$$
\begin{aligned}
U(1) &= A_u M, \\
\hat{M}(1) &= A_u^{-1} Y(k) = M + A_u^{-1} W(1). \qquad (19)
\end{aligned}
$$

The dynamics of the Schalkwijk's coding scheme for $k \geq 2$ can be summarized as follows:

$$
\begin{aligned}
U(k) &= \sqrt{A_u^2 - 1} A_u^{k-1} (\hat{M}(k-1) - M), \\
\hat{M}(k) &= \hat{M}(k-1) - A_u^{-k-1} \sqrt{A_u^2 - 1} Y(k), \qquad (20)
\end{aligned}
$$

where $A_u = \sqrt{\frac{P + \sigma_w^2}{\sigma_w^2}}$ and σ_w^2 is the variance of the additive white Gaussian noise in the forward channel.

In our coding scheme, for $k = 1$,

$$
\begin{aligned}
U(1) &= A_u^2 M, \\
\hat{M}(1) &= A_u^{-2} Y(1) = M + A_u^{-2} W(1). \qquad (21)
\end{aligned}
$$

Substituting these selected parameters into (8) and the fourth line of (9), we have channel inputs and the message estimate of our proposed coding scheme as follows:

$$
\begin{aligned}
U(k) &= \sqrt{A_u^2 - 1} A_u^{k} (\hat{M}(k-1) - M), \\
\hat{M}(k) &= \hat{M}(k-1) - A_u^{-k-2} \sqrt{A_u^2 - 1} Y(k). \qquad (22)
\end{aligned}
$$

By scaling the message M and the corresponding estimate $\hat{M}$ by a factor A_u, we recover the dynamics of Schalkwijk's scheme. Note that this constant scaling of the message index M has no effect on the reliable transmission rate and the power cost at the channel input. The proof is complete.

$$\begin{aligned}
H(M|Z_1^n,\tilde{Z}_1^n,\hat{Z}_1^n) \geq & H(M|Z_1^n,\tilde{Z}_1^n,\hat{Z}_1^n,W_1^n,Q_1^n,V_2^n,\tilde{V}_2^n,\hat{V}_2^n)\\
=&H(M|Z_1,\tilde{Z}_1,\hat{Z}_1,W_1^n,Q_1^n,V_2^n,\tilde{V}_2^n,\hat{V}_2^n)\\
=&H(M|A_u^2M+V_1,A_u^2M+\tilde{V}_1+W_1,A_u^2M+\hat{V}_1+W_1,W_1^n,Q_1^n,V_2^n,\tilde{V}_2^n,\hat{V}_2^n)\\
=&H(M|A_u^2M+V_1,A_u^2M+\tilde{V}_1,A_u^2M+\hat{V}_1,W_1^n,Q_1^n,V_2^n,\tilde{V}_2^n,\hat{V}_2^n)\\
=&H(M|A_u^2M+V_1,A_u^2M+\tilde{V}_1,A_u^2M+\hat{V}_1,W_1^n,Q_1^n,V_2^{1+\bar{d}},\tilde{V}_2^{1+\tilde{d}},\hat{V}_2^{1+\hat{d}})\\
=&H(M|A_u^2M+V_1,A_u^2M+\tilde{V}_1,A_u^2M+\hat{V}_1,W_1,Q_1,V_2^{1+\bar{d}},\tilde{V}_2^{1+\tilde{d}},\hat{V}_2^{1+\hat{d}}). \qquad (23)\\
I(M;Z_1^n,\tilde{Z}_1^n,\hat{Z}_1^n) \leq & I(M;A_u^2M+V_1,A_u^2M+\tilde{V}_1,A_u^2M+\hat{V}_1,W_1,Q_1,V_2^{1+\bar{d}},\tilde{V}_2^{1+\tilde{d}},\hat{V}_2^{1+\hat{d}}) = I(M;\mathbb{A}M+\mathbb{B}), \qquad (24)
\end{aligned}$$

D. Proof of Theorem 2

Starting from the decoder with $A_u = 2^r$ and $B_u = -1$, we have the decoding dynamics ($k \geq 2$) given by

$$\begin{aligned}
\hat{X}_u(k) =& A_u\hat{X}_u(k-1) + B_u(Y(k-1)+Q(k-1))\\
=&A_u(A_u\hat{X}_u(k-2)+B_u(Y(k-2)+Q(k-2)))\\
&+B_u(Y(k-1)+Q(k-1))\\
=&A_u^2\hat{X}_u(k-2)+A_uB_u(Y(k-2)+Q(k-2))\\
&+B_u(Y(k-1)+Q(k-1))\\
=&\cdots\\
=&A_u^k\hat{X}_u(0)+B_u\sum_{i=0}^{k-1}A_u^{k-1-i}(Y(i)+Q(i))\\
=&B_u\sum_{i=0}^{k-1}A_u^{k-1-i}(Y(i)+Q(i))\\
=&-\sum_{i=0}^{k-1}2^{r(k-1-i)}(Y(i)+Q(i)).
\end{aligned} \qquad (25)$$

Then, the estimate of the initial state of the encoder (i.e., the message M) is given by

$$\hat{M}(k-1) = A_u^{-k}\hat{X}_u(k) = -\sum_{i=0}^{k-1}2^{-r(i+1)}(Y(i)+Q(i)). \qquad (26)$$

Next, based on (8) with $C_s = 0$ and $C_u = \frac{1}{A_u} - A_u$, we have the dynamics of channel inputs as

$$\begin{aligned}
U(k) =& C_uA_u^k(M-\hat{M}(k-1))\\
=&C_uA_u^k(M-A_u^{-k}\hat{X}_u(k))\\
=&C_uA_u^k\Big[M-A_u^{-k}\Big(A_u\hat{X}_u(k-1)+B_u(Y(k-1)\\
&+Q(k-1))\Big)\Big]\\
=&C_uA_u^k\Big(M-A_u^{-k+1}\hat{X}_u(k-1)\Big)-C_uB_u\Big(Y(k-1)\\
&+Q(k-1)\Big)\\
=&C_uA_u^k(M-\hat{M}(k-2))-C_uB_u\Big(Y(k-1)\\
&+Q(k-1)\Big)\\
=&A_uU(k-1)-C_uB_u\Big(Y(k-1)+Q(k-1)\Big)\\
=&2^rU(k-1)+(2^{-r}-2^r)\Big(Y(k-1)+Q(k-1)\Big).
\end{aligned} \qquad (27)$$

Note that our decoder (26) and encoder (27) are identical to the coding schemes (2) and (4) in [41]. In addition, [41, Th. 3.2] shows that, for a given r_q (Definition 2), the proposed scheme can achieve any transmission rate r with $r < r_q$.

Now, we need to prove that the proposed coding scheme achieves secrecy with regard to the eavesdropper. In fact, we can directly follow the proof of Proposition 2 and characterize the channel inputs as

$$\begin{aligned}
U(1) =& A_u^2\ M, \qquad U(2) = -C_u(W(1)+Q(1)),\\
U(k) =& -C_uA_u^k\Big((1-A_u^{-1}B_uC_u)^{k-2}\frac{W(1)}{A_u^2}\\
&+\sum_{i=2}^{k-1}A_u^{-i-1}(1-A_u^{-1}B_uC_u)^{k-1-i}B_u(W(i)+Q(i))\Big),\\
&k\geq 3.
\end{aligned} \qquad (28)$$

As a consequence, the channel inputs of the proposed coding scheme depend only on the past forward channel noise W and feedback quantization noise Q. This fact enables us to show that, by following the proof of Theorem 1, this coding scheme satisfies the secrecy requirement

$$\lim_{n\to\infty}\frac{1}{n}I(M;Z_1^n,\tilde{Z}_1^n,\hat{Z}_1^n) = 0.$$

To avoid redundancy, we herein only provide a sketch of the arguments. Details can be directly obtained by following the same methodology from (13) to (18). First of all, we have (23), as shown at the top of this page, where in the last line Q_1 depends on $Y_1 = {A_u}^2M + W(1)$. Then, we obtain (24), as shown at the top of this page, where $\mathbb{A} = [A_u^2,\ A_u^2,\ A_u^2,\ \mathbf{0}^T]$ ($\mathbf{0}$ is an $(\bar{d}+\tilde{d}+\hat{d}+2)\times 1$ zero matrix) and $\mathbb{B} = [V_1,\tilde{V}_1,\hat{V}_1,W_1,Q_1,V_2^{1+\bar{d}},\tilde{V}_2^{1+\tilde{d}},\hat{V}_2^{1+\hat{d}}]$. The rest of the proof is omitted as it directly follows from (18).

V. Conclusion

In this paper, we have considered the finite-order ARMA Gaussian wiretap channel with feedback and have shown that the feedback secrecy capacity equals the feedback capacity without the presence of an eavesdropper. We have further extended our scheme to the AWGN channel with quantized

feedback and proved that our scheme can achieve a positive secrecy rate, which converges to the AWGN channel capacity as the quantization noise decreases to zero.

We conclude this paper by pointing out a few related research topics, which can facilitate a greater understanding of secure communication with feedback. First of all, it is known that the *S-K* coding scheme nicely unifies communications, control and estimation for feedback systems. In this paper, by leveraging the tools from both control and communications, we have shown that a variant of the generalized *S-K* scheme automatically provides secrecy for the legitimate users. However, understanding the secrecy nature of the *S-K* scheme from an estimation perspective is missing from this work. One possible investigation along this line is to extend the fundamental relation between the derivative of the mutual information and the minimum mean-square error (MMSE) [42], known as I-MMSE, from open-loop channels to feedback channels by invoking the direct information studied in [37] and [38] rather than the mutual information [43]. Furthermore, extending the current results to channels with noisy feedback is also of interest. Toward this end, it is necessary to first construct a feedback coding scheme with a good positive achievable rate for noisy feedback channels without the presence of an eavesdropper, which itself is quite a challenging problem in general. What is more, we remark that in this paper we have investigated the condition of weak secrecy, i.e., the normalized mutual information at the eavesdropper vanishes as the code block length increases. However, according to (18), one can see that our coding scheme imposes a finite upper bound on the leaking information, i.e., the mutual information between the message and the signals received by Eve. More importantly, this bound is independent from the code length. That is, the level of leaking information scales much slower (in fact, remains as a constant) even when the code length increases. This indicates that the nature of our linear coding scheme leads to a secrecy level approaching to (but not exactly) the strong secrecy. Therefore, it is of further interest to investigate a modified version of the proposed coding scheme in this paper or other coding schemes which can achieve strong or even semantic secrecy for the colored Gaussian channels, and check under which conditions noiseless feedback still offers secrecy for free.

REFERENCES

[1] C. Li and Y. Liang, "Secrecy capacity of the first-order autoregressive moving average Gaussian channel with feedback," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aachen, Germany, Jun. 2017, pp. 1963–1967.

[2] C. Li, Y. Liang, H. V. Poor, and S. Shamai, "A coding scheme for colored Gaussian wiretap channels with feedback," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Vail, CO, USA, Jun. 2018, pp. 131–135.

[3] C. Shannon, "The zero error capacity of a noisy channel," *IRE Trans. Inf. Theory*, vol. 2, no. 3, pp. 8–19, Sep. 1956.

[4] P. Elias, "Channel capacity without coding," *Inst. Radio Eng.*, vol. 45, no. 3, pp. 381–381. 1957.

[5] P. Elias, "Networks of Gaussian channels with applications to feedback systems," *IEEE Trans. Inf. Theory*, vol. 13, no. 3, pp. 493–501, Jul. 1967.

[6] J. Schalkwijk and T. Kailath, "A coding scheme for additive noise channels with feedback—I: No bandwidth constraint," *IEEE Trans. Inf. Theory*, vol. 12, no. 2, pp. 172–182, Apr. 1966.

[7] J. Schalkwijk, "A coding scheme for additive noise channels with feedback–II: Band-limited signals," *IEEE Trans. Inf. Theory*, vol. 12, no. 2, pp. 183–189, Apr. 1966.

[8] S. Butman, "A general formulation of linear feedback communication systems with solutions," *IEEE Trans. Inf. Theory*, vol. IT-15, no. 3, pp. 392–400, May 1969.

[9] S. Butman, "Linear feedback rate bounds for regressive channels," *IEEE Trans. Inf. Theory*, vol. 22, no. 3, pp. 363–366, May 1976.

[10] J. Wolfowitz, "Signalling over a Gaussian channel with feedback and autoregressive noise," *J. Appl. Probab.*, vol. 12, no. 4, pp. 713–723, 1975.

[11] L. H. Ozarow, "Random coding for additive Gaussian channels with feedback," *IEEE Trans. Inf. Theory*, vol. 36, no. 1, pp. 17–22, Jan. 1990.

[12] L. H. Ozarow, "Upper bounds on the capacity of Gaussian channels with feedback," *IEEE Trans. Inf. Theory*, vol. 36, no. 1, pp. 156–161, Jan. 1990.

[13] T. M. Cover and S. Pombra, "Gaussian feedback capacity," *IEEE Trans. Inf. Theory*, vol. 35, no. 1, pp. 37–43, Jan. 1989.

[14] Y.-H. Kim, "Feedback capacity of stationary Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 57–85, Jan. 2010.

[15] A. Gattami. (Nov. 21, 2015). "Feedback capacity of Gaussian channels revisited." [Online]. Available: https://arxiv.org/abs/1511.06866

[16] C. Li and N. Elia, "Youla coding and computation of Gaussian feedback capacity," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 3197–3215, Apr. 2018.

[17] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[18] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[19] D. Gunduz, D. R. Brown, and H. Vincent Poor, "Secret communication with feedback," in *Proc. Int. Symp. Inf. Theory Appl.*, Auckland, New Zealand, Dec. 2008, pp. 1–6.

[20] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with secure rate-limited feedback," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5353–5361, Dec. 2009.

[21] L. Lai, H. El Gamal, and H. V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5059–5067, Nov. 2008.

[22] G. T. Amariucai and S. Wei, "Feedback-based collaborative secrecy encoding over binary symmetric channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 8, pp. 5248–5266, Aug. 2012.

[23] B. Dai, Z. Ma, and L. Yu, "Feeding back the output or sharing state, which is better for the state-dependent degraded wiretap channel with noncausal CSI at the transmitter?" *Entropy*, vol. 17, no. 12, pp. 7900–7925, 2015.

[24] B. Yang, W. Wang, Q. Yin, and J. Fan, "Secret wireless communication with public feedback by common randomness," *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 269–272, Jun. 2014.

[25] B. Dai, A. J. H. Vinck, and Y. Wang, "Feedback enhances the security of wiretap channel with states," *AEU - Int. J. Electr. Commun.*, vol. 69, no. 7, pp. 1047–1057, 2015.

[26] X. He and A. Yener, "The role of feedback in two-way secure communications," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8115–8130, Dec. 2013.

[27] G. Bassi, P. Piantanida, and S. Shamai (Shitz), "On the capacity of the wiretap channel with generalized feedback," in *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, Jun. 2015, pp. 1154–1158.

[28] B. Dai and Y. Luo, "An improved feedback coding scheme for the wire-tap channel," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 1, pp. 262–271, Jan. 2019.

[29] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Multiple access channels with generalized feedback and confidential messages," in *Proc. IEEE Inf. Theory Workshop*, Tahoe City, CA, USA, Sep. 2007, pp. 608–613.

[30] B. Dai and Z. Ma. (Sep. 28, 2017). "Multiple access wiretap channel with noiseless feedback." [Online]. Available: https://arxiv.org/pdf/1701.04052.pdf

[31] R. Ahlswede and N. Cai, "Transmission, identification and common randomness capacities for wire-tape channels with secure feedback from the decoder," in *General Theory of Information Transfer and Combinatorics*, Berlin, Germany: Springer, 2006, pp. 258–275.

[32] X. Li, B. Dai, and Z. Ma, "How can we fully use noiseless feedback to enhance the security of the broadcast channel with confidential messages," *Entropy*, vol. 19, no. 10, p. 529, 2017.

[33] T. T. Kim and H. V. Poor, "The Gaussian wiretap channel with noisy public feedback: Breaking the high-SNR ceiling," in *Proc. Conf. Rec. 43rd Asilomar Conf. Signals, Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2009, pp. 819–823.

[34] S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai (Shitz), "Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5244–5256, Sep. 2013.
[35] R. Tandon, P. Piantanida, and S. Shamai (Shitz), "On multi-user MISO wiretap channels with delayed CSIT," in *Proc. IEEE Int. Symp. Inf. Theory*, Honolulu, HI, USA, Jun./Jul. 2014, pp. 211–215.
[36] N. Elia, "When bode meets Shannon: Control-oriented feedback communication schemes," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1477–1488, Sep. 2004.
[37] J. L. Massey, "Causality, feedback and directed information," in *Proc. Int. Symp. Inf. Theory and Its Appl.*, Waikiki, HI, USA, 1990, pp. 303–305.
[38] G. Kramer, "Directed information for channels with feedback," Ph.D. dissertation, Swiss Federal Inst. Technol., Zurich, Switzerland, 1998.
[39] C. Li and N. Elia, "The information theoretic characterization of the capacity of channels with noisy feedback," in *Proc. IEEE Int. Symp. Inf. Theory*, St. Petersburg, Russia, Jul./Aug. 2011, pp. 174–178.
[40] C. Li and N. Elia, "Upper bound on the capacity of Gaussian channels with noisy feedback," in *Proc. 49th Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Sep. 2011, pp. 84–89.
[41] N. C. Martins and T. Weissman, "Coding for additive white noise channels with feedback corrupted by quantization or bounded noise," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4274–4282, Sep. 2008.
[42] D. Guo, S. Shamai, and S. Verdú, "The interplay between information and estimation measures," *Found. Trends Signal Process.*, vol. 6, no. 4, pp. 243–429, 2012.
[43] H. Asnani, K. Venkat, and T. Weissman, "Relations between information and estimation in the presence of feedback," in *Information and Control in Networks* (Lecture Notes in Control and Information Sciences). vol. 450, G. Como, B. Bernhardsson and A. Rantzer, Ed. Cham, Switzerland: Springer, 2014.

Chong Li (S'08–M'13) is a Co-Founder of Nakamoto & Turing Labs based in New York City. He is also an adjunct assistant professor at Columbia University (in the City of New York). Prior to that, he was a staff research engineer at Qualcomm. Dr. Li received a Ph.D degree from Iowa State University and a B.E. degree from Harbin Institute of Technology, both in Electrical Engineering. He is a holder of 200+ international/U.S. patents (granted and pending). Dr. Li has been actively publishing papers on top-ranking journals, including PROCEEDINGS OF THE IEEE, IEEE TRANSACTIONS ON INFORMATION THEORY, *IEEE Communications Magazine*, *Automatica*, etc. He has also served as reviewer and technical program committee for most prestigious journals and conferences in communications and control societies. He is the author of the book *Reinforcement Learning for Cyber-physical Systems* (Taylor & Francis CRC press). Dr. Li received MediaTek Inc. & Wu Ta You Scholar Award from MediaTek Inc., Rosenfeld International Scholarship and Research Excellent Award from Iowa State University.

Dr. Li has broad research interests including information theory, blockchain, machine learning, networked control & communications theory, and systems design for advance telecommunication technologies (5G and beyond).

Yingbin Liang (S'00–M'05–SM'16) received the Ph.D. degree in Electrical Engineering from the University of Illinois at Urbana-Champaign in 2005. In 2005-2007, she was working as a postdoctoral research associate at Princeton University. In 2008-2009, she was an assistant professor at University of Hawaii. In 2010-2017, she was an assistant and then an associate professor at Syracuse University. Since August 2017, she has been an associate professor at the Department of Electrical and Computer Engineering at the Ohio State University. Dr. Liang's research interests include machine learning, statistical signal processing, optimization, information theory, and wireless communication and networks.

Dr. Liang was a Vodafone Fellow at the University of Illinois at Urbana-Champaign during 2003-2005, and received the Vodafone-U.S. Foundation Fellows Initiative Research Merit Award in 2005. She also received the M. E. Van Valkenburg Graduate Research Award from the ECE department, University of Illinois at Urbana-Champaign, in 2005. In 2009, she received the National Science Foundation CAREER Award, and the State of Hawaii Governor Innovation Award. In 2014, she received EURASIP Best Paper Award for the *EURASIP Journal on Wireless Communications and Networking*. She served as an Associate Editor for the Shannon Theory of the IEEE TRANSACTIONS ON INFORMATION THEORY during 2013-2015.

H. Vincent Poor (S'72–M'77–SM'82–F'87) received the Ph.D. degree in electrical engineering and computer science from Princeton University in 1977. From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990 he has been on the faculty at Princeton, where he is the Michael Henry Strater University Professor of Electrical Engineering. During 2006 to 2016, he served as Dean of Princeton's School of Engineering and Applied Science. He has also held visiting appointments at several other institutions, most recently at Berkeley and Cambridge. His research interests are in the areas of information theory and signal processing, and their applications in wireless networks, energy systems and related fields. Among his publications in these areas is the recent book *Information Theoretic Security and Privacy of Information Systems* (Cambridge University Press, 2017).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, and is a foreign member of the Chinese Academy of Sciences, the Royal Society, and other national and international academies. Recent recognition of his work includes the 2017 IEEE Alexander Graham Bell Medal, Honorary Professorships from Peking University and Tsinghua University, both conferred in 2017, and a D.Sc. *honoris causa* from Syracuse University awarded in 2017.

Shlomo Shamai (Shitz) (S'80–M'82–SM'89–F'94–LF'18) received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the Technion–Israel Institute of Technology, in 1975, 1981 and 1986 respectively.

During 1975-1985 he was with the Communications Research Labs, in the capacity of a Senior Research Engineer. Since 1986 he is with the Department of Electrical Engineering, Technion–Israel Institute of Technology, where he is now a Technion Distinguished Professor, and holds the William Fondiller Chair of Telecommunications. His research interests encompasses a wide spectrum of topics in information theory and statistical communications.

Dr. Shamai (Shitz) is an IEEE Life Fellow, an URSI Fellow, a member of the Israeli Academy of Sciences and Humanities and a foreign member of the US National Academy of Engineering. He is the recipient of the 2011 Claude E. Shannon Award, the 2014 Rothschild Prize in Mathematics/Computer Sciences and Engineering and the 2017 IEEE Richard W. Hamming Medal. He is a co-recipient of the 2018 Third Bell Labs Prize for Shaping the Future of Information and Communications Technology.

He has been awarded the 1999 van der Pol Gold Medal of the Union Radio Scientifique Internationale (URSI), and is a co-recipient of the 2000 IEEE Donald G. Fink Prize Paper Award, the 2003, and the 2004 joint IT/COM societies paper award, the 2007 IEEE Information Theory Society Paper Award, the 2009 and 2015 European Commission FP7, Network of Excellence in Wireless COMmunications (NEWCOM++, NEWCOM#) Best Paper Awards, the 2010 Thomson Reuters Award for International Excellence in Scientific Research, the 2014 EURASIP Best Paper Award (for the *EURASIP Journal on Wireless Communications and Networking*), the 2015 IEEE Communications Society Best Tutorial Paper Award and the 2018 IEEE Signal Processing Best Paper Award. Dr. Shamai (Shitz) is listed as a Highly Cited Researcher (Computer Science) for the years 2013/4/5/6/7/8. He is also the recipient of 1985 Alon Grant for distinguished young scientists and the 2000 Technion Henry Taub Prize for Excellence in Research. He has served as Associate Editor for the Shannon Theory of the IEEE TRANSACTIONS ON INFORMATION THEORY, and has also served twice on the Board of Governors of the Information Theory Society. He has also served on the Executive Editorial Board of the IEEE TRANSACTIONS ON INFORMATION THEORY and on the IEEE Information Theory Society Nominations and Appointments Committee, and serves on the IEEE Information Theory Society, Shannon Award Committee.